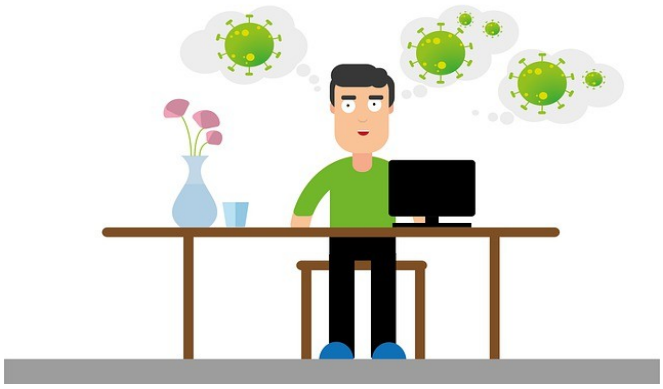
LES NOTES DU CREOGN

Centre de Recherche de l'Ecole des Officiers de la Gendarmerie Nationale

Numéro 59 – Mai 2021

LCL (RC) Patrick MERVENT



COVID-19 ET TÉLÉTRAVAIL : ÉCHANTILLONS DE SOLUTIONS INFORMATIQUES SÉCURISÉES

I) État des lieux

La situation de crise et de confinement liée à l'épidémie de Covid-19 engendre une intensification du recours au télétravail et aux modalités de réunion virtuelle. Certaines entreprises étaient déjà plus ou moins préparées au télétravail, mais pas pour y faire face de manière aussi massive et sur un temps aussi long. La pression gouvernementale se fait toujours plus forte pour que le télétravail devienne la règle, chaque fois que c'est possible.

Dans ces conditions, les salariés se sentent parfois isolés au travail et même coupés des autres. Dans certains cas, notamment dans les petites structures, faute d'avoir pu déployer les moyens nécessaires, le télétravail s'opère depuis les équipements personnels des collaborateurs, dont le niveau de sécurité ne peut pas être évalué et encore moins garanti.

Or, à l'image d'une chaîne, la sécurité d'un système informatique s'évalue au niveau de sécurité du maillon le plus faible. Ainsi, une porte blindée est inutile dans un bâtiment si les fenêtres sont ouvertes sur la rue et plus le bâtiment est grand et complexe, plus les opportunités d'effraction sont nombreuses. Ainsi, une grande entreprise travaillant avec des petites et moyennes entreprises (PME) qui autorisent le télétravail avec du matériel personnel, s'expose elle-même à bien des dangers.

II) Évaluation de la situation et de la menace

Comme nous l'avons vu plus haut, le risque le plus prégnant et évident concerne l'usage des équipements informatiques personnels du salarié pour exécuter son travail, une pratique appelée « BYOD » : *« Bring your own device »* (« apportez votre équipement personnel »). La cohabitation des usages privés et professionnels sur un même terminal doit être envisagée avec circonspection. Si l'utilisation d'un seul équipement dans les deux contextes ne peut être évité, notamment en raison des carences matérielles, il convient de mettre en œuvre des solutions dédiées, proposées par l'employeur, pour cloisonner efficacement chaque environnement (personnel, professionnel), en étant vigilant sur les niveaux de sécurité des solutions du marché. Il est illusoire d'espérer atteindre un haut niveau de sécurité avec un smartphone ou une tablette ordinaire personnels, quel que soit leur paramétrage. Il est par ailleurs plus que délicat pour l'entreprise d'exercer un contrôle ou d'intervenir sur des équipements personnels.

L'employeur étant responsable de la sécurité des données personnelles de son entreprise, cette responsabilité s'applique également lorsque ces données sont stockées sur le matériel informatique personnel du salarié. L'employeur doit donc prendre les mesures nécessaires contre les risques relatifs à la confidentialité des

données, aux intrusions, aux virus. Avec la mise en place du Règlement général sur la protection des données (RGPD), la pratique du BYOD est de plus en plus encadrée et implique pour l'employeur de revoir l'ensemble de sa politique organisationnelle. Pratiquer le BYOD, qu'il s'agisse d'un choix ou d'une contrainte dans le cas du télétravail imposé par la pandémie, nécessite d'appliquer un ensemble de bonnes pratiques pour se conformer à la réglementation européenne. L'employeur doit être en capacité de protéger et de récupérer les données, notamment en cas de perte ou de vol du matériel ou en cas de départ du salarié.
Il est à noter que l'Agence nationale de la sécurité des systèmes d'information (ANSSI) n'est pas favorable au BYOD, même si les fabricants et les éditeurs spécialisés multiplient les solutions pour sécuriser les équipements en séparant hermétiquement environnement personnel et professionnel au sein du même terminal (Good Technology, Blackberry Balance, Samsung Knox, etc.). Le BYOD a favorisé l'usage de systèmes d'information et d'applications informatiques non homologués par les Directions des systèmes d'information (DSI), ce que l'on appelle le shadow IT. Le shadow IT et le télétravail peuvent mettre en danger toute l' activité de l'entreprise face à une cybercriminalité qui redouble d'efforts pour profiter de ces nouvelles opportunités.

III) Principes généraux de sécurité informatique applicables au télétravail

Pour assurer cette transition vers un télétravail en toute sécurité, une tendance qui se pérennise au-delà de la crise sanitaire, il y a une règle absolue en informatique nommée « Disponibilité, Intégrité, Confidentialité, Preuve » (DICP – ou DICT pour « Traçabilité »).
Afin que le télétravailleur puisse produire efficacement à distance, il faut évidemment que ses données de travail soient disponibles, notamment l'accès au partage avec les autres collaborateurs.
Pour préserver la confidentialité, il faut sans conteste proscrire l'usage du shadow IT qui constitue une fenêtre ouverte sur l'entreprise, pour sélectionner une solution complète[2] et s'assurer que seules les personnes autorisées aient accès aux ressources échangées.

L'intégrité des données doit être préservée des attaques par logiciels ou actions malveillants. Enfin, par preuve (ou traçabilité), on vise à garantir qu'aucun des intervenants ne pourra nier sa participation aux échanges, par l'enregistrement des logs[3].

Parmi les parades à déployer pour contrer les attaques, il est nécessaire de mettre en place au moins cinq principes :

- le cloisonnement des parties de l'outil personnel ayant vocation à être utilisées dans un cadre professionnel (création d'une « bulle de sécurité ») ;

- le contrôle d'accès distant par un dispositif d'authentification robuste de l'utilisateur (si possible à l'aide d'un certificat électronique, d'une carte à puce, authentification double facteur) ;

- des mesures de chiffrement des flux d'informations (VPN, HTTPS, etc.). Le chiffrement VPN (*Virtual Private Network*, en français « réseau privé virtuel ») permet de connecter les employés en télétravail comme s'ils étaient directement raccordés au réseau local Intranet de l'entreprise. Il protège le trafic Internet et masque l'identité en ligne, notamment lorsque le salarié accède au système d'information de l'entreprise par une box Internet personnelle dont le mot de passe n'est pas complexe ou encore à travers un *hotspot* WiFi public dont l'accès n'est pas sécurisé. Lorsqu'on se connecte par VPN, le trafic Internet passe à travers un tunnel chiffré à l'intérieur duquel personne ne peut voir les données qui transitent, pas même le fournisseur d'accès Internet. Sans chiffrement VPN, un tiers mal intentionné peut intercepter toutes les données transitant sur le réseau, notamment l'identifiant et le mot de passe du salarié. Il permet au pirate de se connecter au réseau de l'entreprise en utilisant ses codes de connexion. Ce piratage se nomme « l'homme du milieu » (HDM) ou « Man-in-the-Middle attack » (MITM). Il permet au pirate de se connecter au réseau de l'entreprise en échappant au contrôle en utilisant les codes de connexion du salarié ;

2 Lors du confinement, beaucoup d'entreprises ont ainsi migré leur informatique sur Microsoft Teams, offrant des prestations essentielles au télétravail et à la règle DCIP.

3 Enregistrement horodaté d'un événement.

- des procédures de secours en cas de panne/perte du terminal personnel (information de l'administrateur réseau, mise à disposition d'un équipement alternatif professionnel, effacement à distance des données professionnelles stockées sur le terminal personnel) ;

- le respect de mesures de sécurité élémentaires telles que le verrouillage du terminal avec un mot de passe conforme aux bonnes pratiques et l'utilisation d'un antivirus à jour.

IV) L'authentification

À l'instar des solutions grand public, comme celle qui génère une alerte lors d'une connexion à un compte Gmail avec un appareil qui n'est pas le sien, on peut imaginer cette solution pour aviser l'utilisateur d'un problème d'usurpation de compte en entreprise. Ceci repose sur la collecte des informations d'adresse MAC (*Media Access Control*) pour un ordinateur ou du numéro IMEI (*International Mobile Equipment Identity*) pour un smartphone. Ce sont des numéros d'identification uniques, sortes de plaque d'immatriculation des appareils électroniques.

À la différence de l'adresse IP qui permet d'identifier son appareil sur Internet et qui varie selon les réseaux de connexion, l'adresse MAC ou le numéro d'IMEI ne changent jamais. Ce système de filtrage par adresse MAC ou numéro d'IMEI n'interdit pas la connexion avec un appareil qui n'est pas celui usuellement utilisé par le salarié. C'est un système de surveillance qui permet d'aviser l'utilisateur d'une intrusion potentiellement malveillante de ses données d'accès à l'entreprise. Il faudrait obligatoirement que l'ordinateur ou le smartphone ait déjà été utilisé pour se connecter afin de valider la chaîne d'authentification.

Pour avoir un contrôle plus solide, il faut passer par une authentification à double facteur (vérification en deux étapes). À l'authentification identifiant/mot de passe, on ajoute l'envoi d'un SMS à usage unique sur le téléphone portable du salarié, pour une connexion par ordinateur, avant d'autoriser l'accès à la ressource. Ceci implique l'interdiction de toute connexion à distance par smartphone, car le code de la double identification arriverait sur le même matériel que celui qui tente de se connecter. Cette authentification renforcée permet de s'assurer que c'est bien le salarié, et pas un tiers ayant dérobé les identifiants, qui se connecte au système d'information de l'entreprise, avant d'autoriser l'accès. Cependant, même si cette méthode est déjà robuste, des hackers particulièrement chevronnés ont montré que des failles du réseau de télécommunications (via le protocole Signaling System #7, ou SS7) permettent d'intercepter des SMS envoyés à un numéro. Dans une démonstration, un pirate a montré qu'il n'a besoin que de quelques informations (nom, prénom, adresse e-mail et numéro de téléphone de la cible) pour contourner le système.
Des plateformes en accès libre sur Internet sont capables d'établir une surface d'attaque détaillée d'une personne ou d'une organisation en collectant ce type d'informations.

Aussi, l'authentification à facteurs multiples ou authentification multi-facteurs, exigeant plus de deux preuves d'identité, complexifie la tâche des hackers.
Un facteur d'authentification – ou une preuve – est une catégorie d'informations servant à vérifier l'identité de l'utilisateur. Chaque facteur supplémentaire augmente l'assurance qu'une entité se livrant à une quelconque communication ou demandant l'accès à un système est bien la personne ou l'organisme qu'elle prétend être. Les trois catégories les plus courantes sont les facteurs mémoriels, les facteurs matériels et les facteurs corporels :

- facteurs mémoriels : ce sont les informations personnelles qu'un utilisateur doit fournir pour se connecter (noms d'utilisateur ou identifiants, mots de passe, codes PIN et réponses aux questions secrètes) ;

- facteurs matériels : ils désignent les éléments qu'un utilisateur doit avoir en sa possession pour se connecter[4] ;

4 Par exemple, les *tokens* (ou jetons de sécurité) : ce sont de petits dispositifs matériels portés par l'utilisateur pour obtenir l'accès à un service réseau. Ils peuvent prendre la forme d'une carte à puce ou être intégrés dans un objet facilement transportable, tel qu'un porte-clé ou une clé USB. Les *tokens* constituent le facteur matériel historique de l'authentification multiple. Cependant, les jetons logiciels deviennent plus courants que les dispositifs matériels. Les *tokens* logiciels sont des applications qui génèrent un code PIN de connexion à usage unique. Les jetons logiciels servent souvent pour l'authentification multiple mobile, dans laquelle c'est l'appareil

Pour l'authentification mobile, un smartphone fournit souvent le facteur matériel, associé à un application générant un mot de passe à usage unique ;

- facteurs corporels : il s'agit des caractéristiques biologiques de l'utilisateur qui sont vérifiées au moment de la connexion. Cette catégorie comprend toutes les méthodes d'authentification biométrique, empreinte de l'iris, empreinte digitale, empreinte du réseau veineux, empreinte palmaire ou du lobe de l'oreille, reconnaissance faciale, reconnaissance vocale.

Il existe en complément des facteurs de localisation spatio-temporelle pour renforcer l'authentification. La localisation actuelle de l'utilisateur peut facilement être vérifiée, la plupart des smartphones étant équipés d'un GPS. Une connexion à partir d'un pays étranger pourra générer une alerte, tout comme les banques le réalisent pour les usages des cartes bancaires anormaux (le client d'une banque ne peut pas physiquement utiliser sa carte de retrait aux États-Unis, puis en Russie 15 minutes plus tard).

Les entreprises devront veiller à renforcer leur charte informatique sur l'aspect sécurité et protection des données utilisées et traitées par les salariés en télétravail, notamment sur le respect des prescriptions de la Commission nationale de l'informatique et des libertés.

***

Les travaux pour la nouvelle loi[5] sur la transition énergétique et la crise sanitaire conduisent à une évolution des comportements, y compris dans les méthodes de travail. Parmi le panel de ces transformations, le télétravail et les visioconférences en font partie. Au regard des menaces, comme le montre l'accroissement des infractions numériques touchant à la fois les particuliers, les entreprises et les administrations, le renforcement permanent de la sécurité informatique est un véritable enjeu pour notre société. Mais il convient de garder à l'esprit que les solutions de durcissement des techniques de sécurisation, telles que celles présentées dans cet exposé, ne pourront pas tout prévenir sans une véritable prise de conscience de nos vulnérabilités quotidiennes dans ce nouvel environnement numérique.

Webographie :

- *Site Cybermalveillance.gouv.fr : https://www.cybermalveillance.gouv.fr/*
- *Site de la Commission nationale de l'informatique et des libertés (CNIL) : https://www.cnil.fr/*
- *Site de l'Agence nationale de la sécurité des systèmes d'information (ANSSI): https://www.ssi.gouv.fr/*
- *Site du ministère de l'Économie; des Finances et de la Relance : https://www.economie.gouv.fr/*
- *Site de Microsoft : https://www.microsoft.com/*

***Patrick MERVENT** est lieutenant-colonel de la réserve citoyenne auprès de la gendarmerie des transports aériens.*

lui-même (smartphone, par exemple) qui fournit le facteur matériel.

5 Projet de loi portant lutte contre le dérèglement climatique et renforcement de la résilience face à ses effets – NOR : TREX2100379L/ Bleue-1.